Revista Ciencia UNEMI
Vol. 13, N° 34, Septiembre-Diciembre 2020, pp. 127 - 143
ISSN 1390-4272 Impreso
ISSN 2528-7737 Electrónico

Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del Ecuador

Mario, Chifla-Villón[1*]; Luis, Puma-Aucapiña[2]; Kléber, Villacís-Real[3]

Resumen

La globalización informática a nivel mundial lleva a las Instituciones Públicas de Educación Superior de la República del Ecuador a precautelar la seguridad de la información, de sus activos de información a través de auditorías en los servidores web. La importancia de evaluar la seguridad lógica de estos servidores radica en la relación de seguridad de la información, el análisis y la selección de estándares que permitan una alineación en los controles de seguridad y sus técnicas de validación a través de instrumentos fiables y relevantes. El objetivo de esta investigación es diseñar un instrumento que permita auditar a servidores con aplicaciones web basados en la norma ISO 27002:2013. Para este estudio se consideró una investigación cualitativa descriptiva que permitiera reflejar la actitud humana frente al uso y el control de seguridad de la información, seguridad de activos de información y decretos ejecutivos que llevó al análisis de las normas ISO 27002:2013 y NIST 800-53 R4. Se crea un instrumento con 82 ítems con una validez y confiabilidad que lo brinda el focus group y el juicio de expertos, que permite alcanzar planes correctivos de los servidores web, sus vulnerabilidades y la adopción sobre medidas de seguridad para las IES evitando pérdidas económicas o retraso en la entrega de servicios informáticos lo que podría conllevar a deteriorar la reputación de la organización.

Palabras clave: seguridad de la información, seguridad de activos de información, auditoría de servidores web, ISO 27002, NIST 800-53.

Preparation of an audit instrument that evaluates the logical security applicable in servers in Public Institutions of Higher Education of Zone 5 of Ecuador

Abstract

The globalization of information worldwide has led the Public Institutions of Higher Education of the Republic of Ecuador to protect the security of their information assets through audits of web servers. The importance of evaluating the logical security of these servers lies in the information security relationship, the analysis and selection of standards that allow an alignment in security controls and their validation techniques through reliable and relevant instruments. The aim of this research is to design an instrument that allows auditing servers with web applications based on the ISO 27002:2013 standard. For this study a qualitative descriptive research was considered to reflect the human attitude towards the use and control of information security, information asset security and executive decrees that led to the analysis of the ISO 27002:2013 and NIST 800-53 R4 standards. An instrument with 82 items was created with a validity and reliability provided by the focus group and the judgement of experts, which allows to reach corrective plans of the web servers, their vulnerabilities and the adoption of security measures for the HEIs avoiding economic losses or delays in the delivery of IT services which could lead to the deterioration of the reputation of the organisation.

Keywords: information security, information asset security, web server audit, ISO 27002, NIST 800-53.

Recibido: 03 de junio de 2020
Aceptado: 07 de septiembre de 2020

[1] Estudiante de Maestría en Auditoría de Tecnologías de Información; Universidad Espíritu Santo – Ecuador; mchifla@uees.edu.ec; https://orcid.org/0000-0001-6535-4617

[2] Estudiante de Maestría en Auditoría de Tecnologías de Información; Universidad Espíritu Santo – Ecuador; luispuma@uees.edu.ec

[3] Magister en Auditoría en Tecnologías de la Información; Universidad Espíritu Santo – Ecuador; kvillacis@uees.edu.ec

*Autor para correspondencia: mchifla@uees.edu.ec

I. INTRODUCCIÓN

En las últimas dos décadas, la innovación tecnológica, la competencia desarrollada en los mercados de telecomunicaciones luego de las privatizaciones y apertura, el despliegue de redes de infraestructura y la convergencia, han permitido que una mayor cantidad de personas estén integradas y conectadas mediante las Tecnologías de la Información y Comunicación (TIC) no sólo a nivel de su región o país sino con el mundo (Ponce Regalado y Rojas Sifuentes, 2010).

De acuerdo con Nugroho (2014) en los hogares latinoamericanos las desigualdades se presentan en dos dimensiones. La primera dimensión hace referencia al retardo que tienen en comparación con los países desarrollados. La segunda dimensión, hace referencia a diversos factores, citando algunos: niveles de remuneración salarial, ubicación geográfica entre otros. En vista de estas descompensaciones la Red Latinoamericana de Portales Educativos (RELPES), en cooperación de 16 países de la región, optaron por el uso de las TICs en la educación con el fin de superar la brecha digital. Países como Costa Rica, Chile, Brasil y México son pioneros en la implementación de Informática Educativa (Sunkel, 2006). Si bien es cierto que las TICs no se pueden desarrollar de forma uniforme en todos los países ni en sus regiones, en América Latina, particularmente el Ecuador se ha contemplado un incremento en el uso de las TICs como lo denota el Instituto Nacional de Estadística y Censos (INEC) en específico el uso de computadoras, acceso a internet (área urbana, rural y nacional), uso de teléfonos inteligentes, frecuencia de uso de internet, de igual manera se ha visto un decremento del analfabetismo digital entre otros (Instituto Nacional de Estadísticas y Censos, 2017).

En las Instituciones de Educación Superior (IES) de América Latina, la Conferencia de Universidades Españolas (CRUE) ha realizado un estudio en el cual participaron 41 universidades enfocándose en la Enseñanza – Aprendizaje, Investigación, Procesos de Gestión, Gestión de la Información, Formación y Cultura de TI y Organización de las TI (Fernández Martínez y Llorens, 2013). La evaluación se realizó mediante el Modelo de Gobierno de TI para las Universidades (GTI4U) que se basa en la Norma de la Organización Internacional de Estandarización (ISO) 38500, la cual establece niveles de madurez y un conjunto de buenas prácticas con indicadores de alto grado de exigencia para el cumplimiento (Organization International Standarization, 2015). Los resultados obtenidos muestran que en la región existe un sólido punto de inicio para posteriores políticas globales de desarrollo universitarias, una alineación de los objetivos de TI con los objetivos de la organización, posibles mejoras sin aumento de gastos en TI, situándolas en un nivel de madurez cercano al 2 (Repetible: El principio está inmaduro, aunque los procesos de Gobierno de TI siguen un patrón regular) según la escala de madurez propuesta por GTI4U (Gumbau Castelló, 2016). Como lo expone Morales Carrillo, Avellán Zambrano, Mera Cantos, y Zambrano Bravo (2019) cuanto más se extienda el uso de Internet en nuestro país y se aumente la dependencia a las infraestructuras y tecnologías informáticas, el nivel de vulnerabilidad se incrementará, por tal motivo aparece la disciplina de la seguridad de la información. De acuerdo con Da Veiga y Eloff (2007), la seguridad de dicha información engloba la tecnología, los procesos y las personas con el propósito de mitigar las amenazas a la información, empleando diferentes medidas técnicas, entre los cuales existen: software especializado en antivirus y antispyware, dispositivos biométricos hasta llegar a los firewalls. Para una correcta gestión de la seguridad de la información se debe adoptar alguna norma o estándar que sea probado por organismos internacionales, por ejemplo: ISO 27000, NIST SP entre otros.

Existe registros de ataques cibernéticos perpetrados exitosamente a nivel mundial con costos que superan los 575.000 millones de dólares a nivel mundial, siendo Latinoamérica afectada por un monto de alrededor de 90.000 millones de dólares; las organizaciones que han sido atacadas tienen diferentes giros de negocio como es el caso de las distribuidoras de gas (Rusia 1982), programas nucleares (Irán 2010), IES (Estados Unidos 2013) entre otros. Ante dichos acontecimientos el mundo vio la necesidad de crear protecciones, normas, leyes que condenen dichos actos. En la región de Latinoamérica, conformada por 20 países, se ha visto un especial énfasis en la creación de estrategias de ciberseguridad. Siendo los pioneros Colombia, Panamá, Paraguay, Chile y Costa Rica que tienen como factor denominador la protección de la

privacidad, respuestas a ataques y socialización de la ciberseguridad (Hernández, 2018).

Las IES del Ecuador que, de acuerdo con lo estipulado en las normas técnicas de control interno según el Acuerdo de la Contraloría General del Estado 39 Registro Oficial Suplemento 87 de 14-dic-2009 Ultima modificación: 30-jun-2016 Estado: Reformado, indican en el Grupo 410 correspondiente a Tecnología de la información, que la Unidad Tecnológica de Información es la responsable de que las actividades y procesos de tecnología de información estén regularizadas y estandarizadas. De igual manera en el subgrupo 10 de Seguridad de tecnología de Información (410-10), la unidad tecnológica de información será la encargada de implementar y administrar las seguridades de tipo hardware y software con el afán de corregir las vulnerabilidades e incidentes de seguridad identificados con el objetivo de proteger y salvaguardar la información (Contraloría General del Estado, 2016). Además, siguiendo el cumplimiento de las leyes, el acuerdo ministerial nro. 166 decreta que la seguridad de la información, la Seguridad Informática y de las Tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información" (Secretaria Nacional del Ecuador - Administración Pública., 2013).

La Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) realizó el estudio de la seguridad de la información en las IES del Ecuador (Pineda, Córdova, y Pérez, 2014), a partir de una muestra de once IES, 55% del sector privado y 45% del sector público. El 82% no dispone de presupuestos exclusivos para seguridad de información, el 91% no cuenta con líneas de investigación en seguridad de la información y las IES que disponen de seguridad la información utilizan la familia de las norma ISO 27000. Dichas falencias han provocado que las IES sean objetivos de ciberataques entre los cuales se destacan: malware, accesos no autorizados a sistemas o información, phishing, suplantación de identidad, denegación de servicios e incumplimientos de políticas de seguridad de la información. Históricamente la infraestructura de TI debía ser propia, encargada de velar por el mantenimiento, configuración, seguridad de la información y de los dispositivos físicos. Como lo indica Pourzargham (2015) como parte esencial de la infraestructura los servidores cumplen trabajos específicos dentro de la organización; siendo de varios tipos por ejemplo de bases de datos, ftp, email y el más sensible el web.

Como lo explica Li y Xue (2014) las organizaciones han optado por contratar servicios de proveedores de servicios de nube para reducir los costos, la utilización de servicios de plataformas web, teniendo como características que su uso se expande a nivel mundial, se puede emplear para intercambio de información de tipo pública o confidencial, entregar servicios, acceso remoto, compatibilidad multiplataforma entre las más importantes; sin dejar al lado el tema de la seguridad de la información que era total responsabilidad de la organización ahora pasa a ser compartida con el proveedor de servicios debido a que las aplicaciones son creadas por humanos y pueden existir vulnerabilidades indetectables, así también la seguridad lógica del servidor puede estar comprometida teniendo puertos abiertos innecesariamente, configuraciones por defecto entre otras, lo que permite explotar vulnerabilidades. De acuerdo con Kavis (2014) la seguridad no está completa si no se aplica una auditoría, a la cual la define como la solución completa para resolver el tema de seguridad porque se encarga de la seguridad y cumplimiento, cifrado de datos, fortalecimiento del entorno, gestión de copias de seguridad y recuperación entre otras actividades con el fin de mantener la triada confidencialidad, integridad y disponibilidad (CID) de la información. Los auditores son los responsables de validar que sus clientes aborden adecuadamente una colección de controles y procesos para recibir un sello de aprobación para satisfacer los requisitos de un conjunto dado de restricciones según lo definido por un conjunto de leyes que gobiernan. Los auditores lo deben realizar basándose en los diferentes estándares existentes, por ejemplo: ISO27001, ISO 27002, SSAE-16, Directive 95/46/ec, Directive 2002/58/ec, SOX, PCI DSS, HIPAA, FedRAMP, FIPS, FERPA.

Para esta investigación se diseñará un instrumento que permite evaluar la seguridad lógica de los servidores web basados en la norma ISO

27002.

II. REVISIÓN DE LA LITERATURA

Seguridad de la Información

Como lo indica Kritzinger y Smith (2008) las organizaciones manejan diversos activos siendo la información parte de los activos importantes. Dicho eso, se la debe blindar con obligatoriedad debido a que algunas organizaciones son las proveedoras de ingresos económicos, ayudan a tener cierta ventaja competitiva y diferenciándolas del resto de compañías (Kumah, Yaokumah, y Okai, 2019); entonces aparece el término de seguridad de la información: el cual se encarga de proteger a la información garantizando la disponibilidad, confidencialidad y la integridad de la información (Aljifri y Navarro, 2003, citado por Kritzinger y Smith, 2008). Por otro parte, Da Veiga y Eloff (2007) concuerdan que la seguridad de la información engloba a tecnología, procesos y personas con el propósito de mitigar las amenazas a la información, empleando diferentes medidas técnicas, citando algunas: software especializado en antivirus y antispyware, dispositivos biométricos hasta llegar a los firewalls.

Así mismo Lewis (2000) citado por Kritzinger y Smith (2008) define a la gestión de la información como la encargada de mantener libre de riesgos, amenazas y vulnerabilidades a la seguridad de la información, dichas prácticas deben ser integradas a las labores diarias. Parte fundamental para lograr lo mencionado es la creación de conciencia en todos los miembros de la organización; la alta gerencia debe encargarse de la aprobación de las políticas de seguridad y monitorear el cumplimiento.

Seguridad de Infraestructura

Las organizaciones han identificado como punto crítico a la infraestructura de TI debido a que soportan los procesos operativos que ayudan al cumplimiento de los objetivos comerciales; dichas infraestructuras están compuestas por los sistemas y servicios de software básicos y complementarios, activos de hardware, redes informáticas y soporte de servidores, actividades y servicios subcontratado, recursos humanos (Damyanov, 2019). De acuerdo con Pourzargham (2015) los servidores proporcionan servicios específicos dentro de una organización siendo de varios tipos por citar algunos: bases de datos, web, ftp, email entre otros. En esa misma línea, destaca que, brindar seguridad a dichos componentes es tarea difícil para el personal de TI debido a las diversas conexiones que se puede tener dentro de la organización y las personas externas que cumplen algún rol.

Según Sedaghat, Haghparast y Maeen (2018) las organizaciones son las encargadas en la protección de datos y la protección de los recursos de datos que incluye CID de la información y los servicios que con frecuencia se declaran y publican como la tríada de la confidencialidad, integridad y disponibilidad (CID). Con el propósito de evitar intrusiones a la seguridad que pueden llevar a la pérdida, eliminación o sustracción de la información personal o empresarial, existen casos documentados que indican cómo fue vulnerada la seguridad y sus consecuencias, pudiendo mencionar: (a) Monster, un portal de trabajo fue pirateado y la información privada de más de 1.3 millones de personas fue robada en 2007; (b) FlexiScale, proveedor de servicios en la nube; un ingeniero eliminó uno de los principales volúmenes de almacenamiento y quedaron sin servicios hasta recuperar toda la información; (c) Zoho, el error de un usuario provocó que se pueda leer los documentos de otros usuarios de una manera desconocida; (d) un recaudador de impuestos alcanzó involuntariamente cientos de archivos de impuestos privados.

Auditoría

Desde la posición de Allinson (2001) el término de auditoría se acostumbraba a relacionarlo con la disciplina de contabilidad y vincularse a la comprobación de la fiabilidad financiera de una organización, sin embargo, con el pasar del tiempo la auditoría se ha convertido en un proceso en el que se mantiene un registro de una serie particular de eventos para proporcionar evidencia en el caso de una disputa, garantizando el cumplimiento de ciertas reglas y regulaciones, además de verificar la efectividad de los sistemas de control y proporcionar evidencia en el caso de actividad criminal los cuales se los conoce como registros de auditoría.

Ciertamente existen diversos criterios para auditoría, pero diversos autores presentan semejanzas al determinar su concepto. Vroom y Von Solms (2004) la definen como "el examen independiente de la información financiera de cualquier entidad, ya sea

con o sin ánimo de lucro, independientemente de su tamaño o forma legal, cuando tal examen es realizado con el fin de expresar una opinión al respecto" (p. 2).

Por consiguiente, la auditoría es un proceso orientado a la seguridad, encargado de revisar que se cumplan las diferentes políticas, controles técnicos, procesos, procedimientos que una organización disponga con el fin de asegurar sus activos críticos.

Para el caso de auditorías de sistema de información (SI), ISACA (2014) define a la auditoría de SI como un proceso que trata de identificar el riesgo y los controles apropiados para mitigar el riesgo a un nivel aceptable. Para Herath y Herath (2014) las auditorías pueden garantizar que los SI estén adecuadamente controlados, sean seguros y funcionen según lo previsto y pueden desempeñar un papel integral en la gestión de riesgos empresariales. La auditoría de SI genera registros digitales y documentación física que se debe recolectar siguiendo los procedimientos adecuados para que la evidencia sea segura, confiable y aceptable desde el plano legal; pudiendo llegar a ser evidencia contundente durante investigaciones de delitos informáticos.

Clasificación de Auditorias.

Como lo expresa Jackson (2010) los tipos de auditorías dependen del análisis que se realice a la arquitectura que se desee intervenir siendo que pueden ser desde una simple opinión hasta unas auditorías completas basadas en la norma ISO 27001 como lo recomienda. La clasificación que indica es: Revisión de seguridad, Evaluación de seguridad y Auditoria de seguridad.

Por otra parte, Onwubiko (2009) indica que al estar conectados permanentemente las vulnerabilidades incrementan como es el hecho de estar conectado a diversas redes, para lo cual ha identificado diferentes auditorías que tienen como objetivo determinar la seguridad de la información y asegurar sus activos críticos. Por consiguiente, la clasificación que indica es: Técnico de sistemas de información, Eficiencia de los sistemas de información, Evaluación de sistemas de información, Evaluación de software, y Auditoría de seguridad de la información.

Además, los autores mencionados indican diversas técnicas con las que se pueden abordar las diferentes auditorías expuestas; dicho eso se puede concluir que existen dos tipos de auditorías, la primera: Revisión técnica de seguridad que se encarga de realizar pruebas de intrusión empleando técnicas de pruebas de penetración, escaneo de vulnerabilidades, análisis de riesgo; la segunda: Auditoría de cumplimiento que tiene por objetivo la revisión de cumplimiento de políticas, normas, estándares y buenas prácticas.

Auditorias de Servidores Web.

Kavis (2014) describe a la auditoría de servidores web como el proceso encargado en la seguridad y cumplimiento, cifrado de datos, fortalecimiento del entorno, gestión de copias de seguridad y recuperación entre otras actividades de los principales servicios con el fin de mantener la confidencialidad, integridad y disponibilidad de la información. Para que la auditoria sea válida debe cumplir con las leyes regionales adoptando alguna norma o estándar certificado, por nombrar algunos: la familia de las ISO27000, SSAE-16, Directive 95/46/ec, Directive 2002/58/ec, SOX, PCI DSS, HIPAA, FedRAMP, FIPS, FERPA, COBIT, ITIL.

Da Silva y De Barros (2017), Kavis (2014), Onwubiko (2009) concuerdan que las familias de las ISO 27000 son las adecuadas para manejar la seguridad.

Estándares

Serie ISO 27000

De acuerdo con Disterer (2013) el estándar fue creado por la asociación de profesionales británicos en 1993 y publicado como las mejores prácticas para la gestión de la seguridad de la información. En el 2005, la Organización Internacional para la Estandarización (ISO) las valoró y fundó la serie ISO 27000 que corresponde a estándares para la creación y operación de sistemas de gestión de seguridad de la información (SGSI). Como lo indica International Organization for Standardization ISO/IEC (2013), ISO 27001 es una de las más aceptadas a nivel mundial por ser un estándar certificable, siendo una guía para gestionar un SGSI que indica controles a emplearse en la seguridad, además permite evaluar el cumplimiento de la norma.

ISO 27002 detalla los requerimientos de la ISO27001, es un complemento que especifica las mejores prácticas de la seguridad de la información para una organización, teniendo en cuenta desde

la seguridad física hasta la seguridad de recursos humanos. Se encuentra estructurada en 14 clausulas, abarca 35 categorías y 114 controles.

NIST SP 800-53

El Instituto Nacional de Normas y Tecnología de los Estados Unidos (National Institute of Standards and Technology - NIST, 2013) publicó un catálogo de controles de seguridad y privacidad para la seguridad de la información llamado NIST SP 800-53 apoyado en la ley federal de administración de seguridad de la información (FISMA), que proporciona, según Jackson (2010), diversos tipos de controles de seguridad para el cumplimiento con los requisitos de seguridad de la información y gestión de riesgos. Tariq et al. (2016) indican que se encuentran divididas en 18 familias con controles según la familia, NIST propone una serie de procesos que gestiona la seguridad de la organización de forma holística tratando la seguridad y protección de los activos, la protección física y ambiental, la gestión de riesgos y especialmente la gestión de programas.

III. METODOLOGÍA

Este estudio toma el método de investigación evaluativa usado para implementación de programas o instrumentos en el área de educación en general incluidas la de Educación Superior a través del planteamiento de objetivos, indicadores y criterios (Martinez Olmo, 2016).

Como medición del resultado alcanzado en esta investigación se trazó el objetivo: Diseñar un instrumento de auditoria que evalúa la seguridad lógica aplicable en servidores en instituciones públicas de Educación Superior de la Zona 5 del Ecuador; en lo cuantificable del objetivo el indicador es la incorporación del 100% de las instituciones públicas de Educación Superior de la Zona 5 y el estándar deseable es la construcción del instrumento con su validación.

Desde el punto de vista funcional la investigación evaluativa cumple con las siguientes actividades:

El propósito y objeto de evaluación es el diseño de un instrumento de auditoria que evalúa la seguridad lógica que se complementa al objeto de evaluación que son los servidores web de las instituciones públicas de Educación Superior de la Zona 5 conformadas por: a) Universidad Estatal de Milagro; b) Universidad Técnica de Babahoyo; c) Universidad Técnica Estatal de Quevedo; d) Universidad Estatal de Santa Elena y e) Universidad Estatal de Bolívar. Son consideradas por la similitud en sus procesos académicos y administrativos que son regulados por Consejo de Educación Superior (CES), Ley Orgánica de Educación Superior (LOES), Ley Orgánica de Servicio Público (LOSEP) y el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES). Estos encuentros permiten crear la primera versión del instrumento.

Las audiencias y el juico a emitir se desarrollan a través de: a) Focus group y b) Juicios de expertos, estas son técnicas investigativas de carácter cualitativa y de participación.

El Focus group permite congregar a un equipo de profesionales (Roussos, Roussos, y Roussos, 2014); para el estudio se consideran las instituciones públicas de la Zona 5 que analizan sobre temas de seguridad lógica de servidores web, normas para seguridad lógica de servidores web: estructuras y controles de seguridad, infraestructura, networking y se realiza una evaluación a la primera versión de un instrumento para revisión de seguridad lógica de servidores web en Instituciones Públicas de Educación Superior (IES). Y guiado por los investigadores. Para conformar el focus group se desarrollaron tres etapas: a) reclutamiento, a partir de un análisis de perfiles profesionales basados en los temas a tratar y en el conocimiento certificado de actividades académicas por parte de los investigadores; b) moderación, a través de la participación de video conferencia; c) elaboración de informe, que permitió crear una segunda versión proveniente de las observaciones de los participantes.

El Juicio de experto se fundamentó en lo planteado por Escobar-Pérez y Cuervo-Martínez (2008), en cuanto a la participación de profesionales en el área de arquitectura de servidores; seguridad de la información y networking reconocidos en la educación superior quienes aportaron con observaciones y recomendaciones para elaborar una tercera versión del instrumento.

El instrumento diseñado en la tercera versión es el indicador que genera la información para alcanzar planes correctivos de los servidores web, sus vulnerabilidades y la adopción sobre medidas de seguridad para las IES basado en la norma

27002:2013.

Las fuentes de información se basaron en la búsqueda de publicaciones escritas en idiomas de español e inglés; con las palabras claves: "Seguridad de la información", "Seguridad de activos de información", "Auditoría de servidores web", "ISO 27002", "NIST 800-53", intercalación de términos con el tema y el título durante el periodo agosto 2019 – febrero 2020. Existió variedad de aportes como artículos científicos relacionados con el tema que no fueron considerados debido la falta de acceso al documento completo por altos costo.

Modelo de valoración.

Escobar-Pérez y Cuervo-Martínez (2008), presentan los Coeficientes de Concordancia que son un instrumento cuantitativo que permite validar la fiabilidad y relevancia del instrumento de auditoría para evaluar la seguridad lógica de los servidores web de las entidades públicas de Educación Superior de la Zona 5. Se dispone de dos pruebas estadísticas: a) el coeficiente de concordancia de Kendall(W) y b) el coeficiente de concordancia de Kappa.

El coeficiente de concordancia de Kendall se utiliza cuando sus variables son de tipo ordinal que permitió conocer el instrumento de auditoría en concordancia con lo que se evalúa en la seguridad de los servidores web. Se utiliza la escala de orden tipo Likert, en la que cada variable se refleja en el instrumento a través de la medición suficiencia, claridad, coherencia y relevancia; representa un nivel de acuerdo o desacuerdo. Dicho coeficiente está basado en el grado de varianza de la suma de los rangos obtenidos de los diferentes jueces dando como resultado un número que oscila entre 0 y 1, mientras más se acerca a 1 la concordancia se fortalece. Si el resultado es mayor o igual a 0,8 se acepta caso contrario se rechaza.

Desarrollo valorativo

Este estudio toma (Tyler, 1942) del modelo evaluativo por objetivos con el paradigma empírico – analítico.

El proceso de valoración se desarrolló a partir de una serie de actividades definidas en un cronograma con una duración de un semestre (agosto 2019 - febrero 2020). En referencia a la recogida y el análisis de la información se inicia con un acercamiento a la Universidad Estatal de Milagro por existir mayor accesibilidad a la información y lidera la educación superior de la Zona 5. A través de esta Alma Máter se logra el acercamiento con las IES en jornadas de trabajo, se levanta un acta sobre el estado actual de la seguridad de los servidores webs, dando origen a la primera versión del instrumento.

En referencia a la formulación de juicios de valor se desarrolló a través de los criterios de los investigadores con base en las normas gubernamentales para la creación de los indicadores que se acogerán a un plan correctivo en la seguridad de la información en primera instancia. Posterior, se desarrolla la segunda versión a través de focus group y juicio de expertos; y finalmente, la valoración de los resultados del instrumento origina la creación de la última versión que está valorado para ser evaluado como una propuesta de instrumento de auditoría para evaluar la seguridad lógica aplicada a servidores de IES de la Zona 5.

Participantes

Mediante el Decreto Ejecutivo N. 878, publicado en el Registro oficial N. 268 del 8 de febrero del 2008 de la República del Ecuador se establece la creación de nueve zonas administrativas de planificación a cargo de la Secretaría Nacional de Planificación y Desarrollo (SENPLADES), con el fin de identificar las necesidades y soluciones efectivas mejorando las prestaciones de servicios públicos (Secretaria Nacional de Planificación y Desarrollo del Ecuador, 2008). Se crearon nuevos niveles administrativos divididos en zonas, distritos y circuitos a nivel nacional.

Las zonas están conformadas por provincias de acuerdo a su cultura, economía y ubicación geográfica, las nueve zonas se encuentran distribuidas de la siguiente manera:

Tabla 1. Distribución de provincias del Ecuador por zonas

NOMBRE	PROVINCIAS
Zona 1	Esmeraldas, Imbabura, Carchi, Sucumbíos.
Zona 2	Pichincha (a excepción de Quito), Napo, Orellana.
Zona 3	Cotopaxi, Tungurahua, Chimborazo, Pastaza.
Zona 4	Manabí, Santo Domingo de los Tsáchilas
Zona 5	Santa Elena, Guayas (a excepción de Guayaquil, Samborondón y Durán), Bolívar, Los Ríos, Galápagos.
Zona 6	Cañar, Azuay, Morona Santiago
Zona 7	El Oro, Loja, Zamora Chinchipe
Zona 8	Cantones de Guayaquil, Samborondón y Durán
Zona 9	Distrito Metropolitano de Quito.

Al haberse establecido la nueva distribución de las provincias, el Estado ordenó a todas las instituciones estatales asignar sus servicios a las zonas correspondientes. En cuanto a la educación, la Secretaría de Educación Superior, Ciencia, Tecnología e Información (Senescyt) se encargó en la distribución de las 30 Instituciones Públicas de Educación Superior (IES) existentes en el Ecuador.

Para este estudio se tomó como referencia la Universidad Estatal de Milagro (UNEMI), perteneciente a la Zona 5, que se encuentra conformada por a) Universidad Estatal de Milagro; b) Universidad Técnica de Babahoyo; c) Universidad Técnica Estatal de Quevedo; d) Universidad Estatal de Santa Elena y e) Universidad Estatal de Bolívar; debido a la similitud en sus procesos académicos y administrativos que son regulados por Consejo de Educación Superior (CES), Ley Orgánica de Educación Superior (LOES), Ley Orgánica de Servicio Público (LOSEP) y el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES).

Para el estudio se seleccionaron tres profesionales que debían cumplir con los siguientes parámetros: formación académica, plaza de trabajo y experiencia. Los profesionales son ingenieros en sistemas, laboran como directores del área de TI y conocen los recursos operativos de las IES, se dedican a la seguridad de la información. Además de contar con cursos, certificaciones relacionadas con la temática; dos profesionales tienen como experiencia al menos tres años como jefes de área de tecnología de la información y uno dicta catedra en el programa académico de ingeniería de software en una IES. Ver apéndice B.

Elaboración del Instrumento

Cumpliendo con lo estipulado en el acuerdo ministerial Nro. 166 de la Constitución del Ecuador decreta que la seguridad de la información, la Seguridad Informática y de las Tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI); elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información" con el objetivo de mitigar los riesgos, proteger la infraestructura gubernamental de ataques informáticos ha dispuesto la adopción de un estándar de seguridad que garantice la confidencialidad, integridad y disponibilidad (CID) de la información (Secretaria Nacional del Ecuador - Administración Pública., 2013).

Por otra parte, existen varias normas para la seguridad de la información de las cuales se ha seleccionado el estándar del Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos 800-53 r4 debido a que gestiona la seguridad de la organización de forma holística tratando la seguridad y protección de los activos, la protección física y ambiental, la gestión de riesgos y especialmente la gestión de programas.

Con el fin de obtener un instrumento que sirva para evaluar la seguridad lógica de servidores web se procedió a realizar un análisis comparativo de las estructuras de las normas, por un lado, ISO27002:2013 está compuesta por clausulas, categorías, controles y guía suplementaria, NIST se conforma de familia, procedimiento, control y guía suplementaria; resultando ser similares y la

posibilidad de alinear sus controles de seguridad. Además, se realizó un análisis cualitativo de las normas para la selección de los controles a emplear en el diseño del instrumento basado en la situación actual de los niveles de seguridad de los servidores web de la organización. Se obtuvo el primer grupo de controles basados en la norma ISO, posteriormente se procedió a evaluar los diversos controles propuestos del estándar NIST para la alineación de las normas, dando como resultado una primera versión del instrumento que consta de 73 ítems provenientes de 12 cláusulas alineados a las dos normas.

Para darle fortaleza al instrumento se realizó un focus group mediante una videoconferencia en la que participaron los profesionales antes mencionados, se dialogó acerca de la seguridad lógica de servidores web, las normas a emplear: estructura y sugerencia de controles, asimismo, se indicaron los ítems del primer diseño del instrumento. Basados en sus criterios, opiniones y sugerencias, se evidenció la necesidad de crear una nueva versión del instrumento agregando, ajustando y eliminando ítems de diversas cláusulas propuestos en el instrumento con la finalidad de disminuir el sesgo de la investigación.

La segunda versión del instrumento, modificado de acuerdo con las sugerencias del focus group, cuenta con 69 ítems provenientes de 11 cláusulas de las normas alineadas. Luego se procedió a evaluar utilizando la técnica de juicio de expertos, cabe decir que los participantes necesitaron de 8 a 12 días, al finalizar la evaluación los participantes entregaron los resultados con sus respectivas observaciones y recomendaciones. En consecuencia, se elaboró una tercera versión del instrumento conformado por 82 ítems provenientes de 11 cláusulas de las normas alineadas; posteriormente, fue presentado y aceptado por los participantes, revisar la tabla 2.

Tabla 2. Distribución de controles de seguridad del instrumento

CLAUSULA	CONTROLES
Políticas de seguridad	4
Organización de la seguridad de la información	9
Gestión de activos	4
Control de acceso	19
Criptografía	5
Seguridad física y ambiental	4
Seguridad en las operaciones	25
Relaciones con los proveedores	4
Gestión de incidentes de seguridad de la información	5
Aspectos de la seguridad de la información de la gestión de la continuidad del negocio	2
Cumplimiento	1
Total	82

Procedimiento

Como lo indica Escobar-Pérez y Cuervo-Martínez (2008) al crear un instrumento de evaluación, y sin ser particularmente nombrado el recipiente, carece de validez y confiabilidad por lo que se debe aplicar técnicas con el objetivo de hacerlo válido y aplicable. La validez de contenido consiste en qué tan adecuado es el muestreo que hace una prueba del universo de posibles conductas, de acuerdo con lo que se pretende medir (Cohen y Swerdik, 2001, citado por Escobar-Pérez y Cuervo-Martínez, 2008). Una de las técnicas de validación es el juicio de expertos, la cual consiste en una opinión de personas con experiencia y reconocidas como experto en el tema a evaluar, puedan aportar información, evidencia, juicios y valoraciones.

Para aplicar dicha técnica se debe definir un documento con los siguientes características: (1) Definir el objetivo del juicio de expertos; (2); Seleccionar los jueces; (3) Explicitar tanto las dimensiones como los indicadores que está midiendo cada uno de los ítems de la prueba; (4) Especificar el objetivo de la prueba; (5) Establecer los pesos diferenciales de las dimensiones de la prueba; (6)

Diseñar las planillas; (7) Calcular la concordancia entre jueces; y (8) Elaborar las conclusiones del juicio que serán utilizadas para la descripción psicométrica de la prueba.

Es necesario resaltar que se crearon plantillas de calificaciones para que los participantes evalúen cada ítem considerando las respectivas categorías y la escala de calificaciones detalladas, ver tabla 3.

Tabla 3. Categorías a evaluar y escala de calificaciones.

CATEGORÍAS	ESCALA
Suficiencia.	1. No cumple con el criterio.
Claridad.	2. Bajo nivel.
Coherencia.	3. Moderado nivel.
Relevancia.	4. Alto nivel.

Igualmente, se definieron las dimensiones para garantizar la aplicación correcta de los términos. El documento fue creado y distribuido vía correo electrónico con el fin de que los expertos realizaran las evaluaciones pertinentes, emisión de observaciones y recomendaciones.

Al recibir los resultados por parte de los expertos se procedió a tabularlos en hojas de cálculos y para validar el contenido y relevancia del instrumento se aplicaron dos pruebas estadísticas: el coeficiente de concordancia de Kappa y el coeficiente de concordancia de Kendall(W). El coeficiente de concordancia de Kappa se utiliza cuando sus variables son de tipo nominal, es decir, se utiliza únicamente para clasificar la información. Por el contrario, el coeficiente de concordancia de Kendall se utiliza cuando sus variables son de tipo ordinal, en otras palabras necesitan una escala de calificación ordenada, tipo Likert, en la que cada variable representa un nivel de acuerdo o desacuerdo. Dicho coeficiente está basado en el grado de varianza de la suma de los rangos obtenidos de los diferentes jueces dando como resultado un número que oscila entre 0 y 1, mientras más se acerca a 1 la concordancia se fortalece. Si el resultado es mayor o igual a 0,8 se acepta caso contrario se rechaza.

Los resultados revelaron que existe aceptación en múltiples ítems, del mismo modo, producto de las observaciones y recomendaciones se debió realizar ajustes que comprenden agregación, reformulación y eliminación de ítems. Realizados los ajustes correspondientes se obtuvo la tercera versión del instrumento la cual fue aprobada por los expertos.

IV. CONCLUSIONES

Existe la inclinación mundial de publicar información de las organizaciones y prestación de servicios a través de la web. Como lo exponen Morales Carrillo et al (2019) cuanto más se extienda el uso de Internet en nuestro país y se aumente la dependencia a las infraestructuras y tecnologías informáticas, el nivel de vulnerabilidad se incrementará. En tal sentido, las instituciones estatales han fortalecido sus políticas de seguridad de la información como se encuentra estipulado en el acuerdo ministerial Nro. 166 de la Constitución del Ecuador en la que el gobierno ecuatoriano a decretado la adopción de la norma ISO 27002 para la seguridad de la información (Secretaria Nacional del Ecuador - Administracion Pública, 2013). Para la seguridad de la información existen varias normas, siendo una de las más utilizadas la NIST 800-53 (Jackson, 2010; Kavis, 2014; Nicho, 2018). Por consiguiente, el instrumento se basó en la alineación de los controles de seguridad la norma ISO 27002:2013 y NIST 800-53 R4.

Esta investigación alcanza su objetivo de diseñar un instrumento de auditoria que evalúa la seguridad lógica aplicable en servidores en instituciones públicas de Educación Superior de la Zona 5 del Ecuador en fase de valoración y que no se logra evaluar totalmente el proceso por situación tiempo convirtiéndose en una limitante. Por lo que queda para futuras investigaciones su aplicación, analisis, replicas en las IES.

En el proceso de creación del instrumento tal como se menciona en la metodología: la primera consideraba 74 ítems elegidos con base a la situación actual de las IES de la Zona 5 del Ecuador y la revisión bibliográfica. A partir de las observaciones derivadas del focus group se generó la segunda versión del instrumento que sugiere la eliminación de 5 ítems relacionados con las cláusulas de seguridad de los

recursos humanos, seguridad física y ambiental.

En la segunda versión del instrumento se toma la referencia Escobar-Pérez y Cuervo-Martínez (2008) que permite alcanzar la validez y relevancia a través del juicio de expertos, éstos aportan con 26 observaciones vinculadas con las cláusulas de política de la seguridad de la información, organización de la seguridad de la información, gestión de activos, control de acceso, seguridad física y ambiental, seguridad de las operaciones, gestión de incidentes de seguridad de la información; que contribuye a la creación de la versión final compuesta de 82 ítems.

Se encontraron las siguientes limitaciones: en el contexto de las IES del Ecuador, existe escasez de estudios para potenciar la seguridad del sistema operativo del servidor web que forma parte de la arquitectura de los sistemas de gestión informática de las IES y la búsqueda de información en repositorios digitales de revistas científicas de alto impacto sobre ciberseguridad aplicada a las IES, instrumentos o guías así como sistemas de alto volumen de transacciones Morales Carrillo et al (2019).

En referencia a instrumentos es casi nulo la evidencia de instrumentos innovadores ya que en su mayoría son traducciones de normas internacionales que no consideran nuestra realidad contextual.

Otro limitante fue el factor tiempo y el estado de excepción vigente no permitio concluir el estudio con la evaluación del instrumento.

Para futuras investigaciones se recomienda evaluar el instrumento mediante estudios longitudinales de impacto sobre auditoría de seguridad lógica en servidores web. Estos resultados deberían ser compartidos a las IES para su difusión y aplicación.

V. BIBLIOGRAFÍA

Allinson, C. (2001). Information systems audit trails in legal proceedings as evidence. *Computers and Security, 20*(5), 409–421. https://doi.org/10.1016/S0167-4048(01)00513-2

Contraloría General del Estado. (2016). Normas de Control Interno de la Contraloría General del Estado 1. *14-Dic-2009*, 1–79. Retrieved from https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/4160-suplemento-al-registro-oficial-no-87

Da Silva, M. P., & De Barros, R. M. (2017). Maturity Model of Information Security for Software Developers. *IEEE Latin America Transactions, 15*(10), 1994–1999. https://doi.org/10.1109/TLA.2017.8071246

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Damyanov, I. (2019). Corporate information infrastructure - Management aspects. *TEM Journal, 8*(1), 102–106. https://doi.org/10.18421/TEM81-14

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security, 04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez De Contenido Y Juicio De Expertos: Una Aproximación a Su Utilización. *Avances En Medición, 6*, 27–36. Retrieved from http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf

Fernández Martínez, A., & Llorens, F. (2013). UNIVERSITIC LATAM 2014. *Journal of Chemical Information and Modeling, 53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Gumbau Castelló, J. P. (2016). S10 : Modelo de Madurez para una universidad. Retrieved from http://tic.crue.org/wp-content/uploads/2016/07/S10-Modelo-de-Madurez-GTI4U.-V1.pdf

Herath, H. S. B., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems, 57*(1), 54–63. https://doi.org/10.1016/j.dss.2013.07.010

Hernández, J. C. (2018). Estrategias Nacionales de Ciberseguridad en America Latina. *Revista de Estudio En Seguridad Internacional*, 1–8. Retrieved from http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-américa-latina

Instituto Nacional de Estadísticas y Censos, I. (2017). *Contenido Ficha técnica Equipamiento del hogar*. Retrieved from http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2016/170125.Presentacion_Tics_2016.pdf

International Organization for Standardization ISO/IEC. (2013). *Information technology - Security techniques - Code of practice for Information security controls (ISO/IEC 27002:2013, IDT)*. (Second Edi). Retrieved from https://www.iso.org

Jackson, C. (2010). *Network Security Auditing*. Indianapolis: Cisco Press.

Kavis, M. (2014). Architecting The Cloud. In *Architecting The Cloud*. https://doi.org/10.1002/9781118691779

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security, 27*(5–6), 224–231. https://doi.org/10.1016/j.cose.2008.05.006

Kumah, P., Yaokumah, W., & Okai, E. S. A. (2019). A conceptual model and empirical assessment of HR security risk management. *Information and Computer Security, 27*(3), 411–433. https://doi.org/10.1108/ICS-05-2018-0057

Li, X., & Xue, Y. (2014). A survey on server-side approaches to securing web applications. *ACM Computing Surveys, 46*(4), 1–29. https://doi.org/10.1145/2541315

Martinez Olmo, F. (2016). La investigación evaluativa. In A. La Muralla (Ed.), *Metodología de la investigación educativa*. (5th ed.). Madrid: 2015.

Morales Carrillo, J. J., Avellán Zambrano, N., Mera Cantos, J. S., & Zambrano Bravo, M. (2019). Ciberseguridad y su aplicación en las Instituciones de Educación Superior. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 438–448. Retrieved from http://repositorio.espam.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf

National Institute of Standards and Technology - NIST. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. In *NIST Special Publication 800-53 Revision 4* (R4 ed.). https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-53r4

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security, 26*(1), 10–38. https://doi.org/10.1108/ICS-07-2016-0061

Nugroho, H. (2014). Conceptual model of IT governance for higher education based on COBIT 5 framework. *Journal of Theoretical and Applied Information Technology, 60*(2), 216–221. https://doi.org/ISSN: 1992-8645

Onwubiko, C. (2009). A Security Audit Framework for Security Management in the Enterprise. https://doi.org/10.1007/978-3-642-04062-7_2

Organization International Standarization, I. (2015). ISO/IEC 38500:2015 Information technology — Governance of IT for the organization. Retrieved from https://www.iso.org/standard/62816.html

Pineda, J., Córdova, C., & Pérez, E. (2014). *INFORME DE RESULTADOS DE LA "1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA*." 12. Retrieved from www.utpl.edu.ec

Ponce Regalado, F., & Rojas Sifuentes, W. (2010). Promoción y desarrollo de las TIC en América Latina. *Research Report*, 1–14.

Pourzargham, H. (2015). Importance of Security in Database. *IJCSNS International Journal of Computer Science and Network Security, 15*(5), 29–31. Retrieved from http://paper.ijcsns.org/07_book/201505/20150504.pdf

Roussos, J., Roussos, S., & Roussos, A. (2014). El focus group como técnica de investigación cualitativa. *Expert Review of Ophthalmology, 9*(5), 353–354. https://doi.org/10.1586/17469899.2014.964497

Secretaria Nacional de Planificación y Desarrollo del Ecuador. (2008). *Zonas administrativas de planificación del Ecuador*. (878). Retrieved from http://www.planificacion.gob.ec/wp-content/uploads/downloads/2012/08/Decreto-Ejecutivo-878-y-sus-reformas-determina-Zonas-de-Planificación.-Registro-Oficial-Nro.-268.pdf

Secretaria Nacional del Ecuador - Administracion Pública. (2013). *Esquema Gubernamental de Seguridad de la Información EGSI*. 1–47. Retrieved from https://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-InformaciÃ3n.pdf

Sedaghat, F., Haghparast, M., & Maeen, M. (2018). Security and Trust In Cloud Computing: A Survey. *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, 11*(12), 1251–1271. https://doi.org/10.4018/978-1-5225-5634-3.ch062

Sunkel, G. (2006). Las tecnologías de la información y la comunicación (TIC) en la educación en América Latina. Una exploración de indicadores. In *Cepal*. https://doi.org/1680-8983

Tariq, M. I., Tayyaba, S., Ashraf, M. W., Rasheed, H., & Khan, F. (2016). Analysis of NIST SP 800-53 Rev.3 Controls Effectiveness for Cloud Computing. *1st National Conference on Emerging Trends and Innovations in Computing & Technology*, 88–92. Retrieved from https://www.researchgate.net/profile/Muhammad_Tariq26/publication/303315109_Analysis_of_NIST_SP_800-53_Rev3_Controls'_Effectiviness_for_Cloud_Computing/links/573cb05208ae9f741b2eb9f8.pdf

Tyler, R. W. (1942). General statement on evaluation. *Journal of Educational Research, 35*(7), 492–501. https://doi.org/10.1080/00220671.1942.10881106

Vroom, C., & Von Solms, rossouw. (2004). Towards information security behavioural compliance. *Computers and Security, 23*(3), 191–198. https://doi.org/10.1016/j.cose.2004.01.012

ANEXOS

APENDICE A. Instrumento para la revisión de seguridad lógica de servidores web.

Nro.	Ítem
1	PSI01. ¿La organización tiene políticas para la seguridad de la información?
2	PSI02. ¿Las políticas que conforman la seguridad de la información se encuentran debidamente aprobadas por la gerencia, publicadas y socializadas con el personal de la organización?
3	PSI03. ¿Existe evidencia que obligue a los empleados y terceros de la organización a cumplir con las políticas de seguridad?
4	RPS01.¿La política de la seguridad de la información tiene revisiones periódicas planificadas, además de contar con mejoras significativas para asegurar su idoneidad, adecuación y eficacia continua?
5	SGD01. ¿Existe la división de los deberes entre roles y áreas responsables de la seguridad de la información para mitigar actividades inapropiadas?
6	SGD02. ¿Existe un control que verifique modificaciones no autorizadas de las configuraciones de seguridad en los servidores web?
7	SGD03. ¿Se evidencia la utilización de instrumentos, como una matriz RACI, para identificar las personas involucradas en una cada tarea?
8	CAU01.¿Existe algún consejo / autoridades destinados a la seguridad de la información que pueden resolver consultas, incidentes y emergencias?
9	CAU02. ¿Esta designado un responsable de contactar al consejo / autoridades y en que punto del incidente?
10	CGI01. ¿Existe contacto con expertos en seguridad de la información por parte del jefe de departamento de TI?
11	GSP01. ¿La seguridad de la información es relevante en la gestión de proyectos?
12	PDM01. ¿Se revisan las configuraciones de los dispositivos móviles para gestionar los riesgos originados?
13	TTJ01. ¿Se encuentra implementada alguna política o medida de seguridad que proteja la información que se accede, procesa o almacena en los lugares que se realiza teletrabajo?
14	UDA01. ¿La información se encuentra clasificada en función de su valor, requisitos legales, sensibilidad y criticidad para la organización?
15	CLI01. ¿Los servicios se distribuyen en diferentes activos para garantizar la alta disponibilidad tomando en cuenta la confidencialidad, integridad y disponibilidad?
16	MAT01. ¿Los medios que contienen información han sido protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización?
17	TMF01. ¿La organización cuenta con una política de control de accesos en la cual se encuentre establecido, documentado, revisado y aprobado el control de accesos basado en los requisitos del negocio y seguridad de la información?
18	PCA01. ¿Existen una política de control de acceso que supervise a los puertos de comunicación abiertos innecesariamente?
19	ARS01. ¿Se encuentra habilitado el acceso por SSH y puerto RPD?
20	ARS02. ¿Los puertos que se encuentran abiertos se basan en los requerimientos de la organización cumpliendo las políticas de seguridad de la información?
21	RCU01. ¿Existe un proceso formal de altas y bajas de usuarios para modificar o cancelar la asignación de derechos de acceso?
22	RCU02. ¿Se cumple con la política de eliminar los usuarios por defecto?
23	SAU01. ¿La organización dispone de un proceso formal para asignar o cancelar accesos a los usuarios para todos los sistemas y servicios?
24	SAU02. ¿Se asigna los accesos básicos a los nuevos usuarios por defecto?
25	SAU03. ¿Se utiliza un ID de usuario únicos para cada usuario?
26	SAU04. ¿Existen una comunicación eficiente entre el departamento de TI y Recursos Humanos?
27	GAP01. ¿Existen algún proceso que controle y restrinja el uso de derechos de acceso con privilegiado?
28	RCD01. ¿Se realizan revisiones documentadas de los derechos de acceso de los usuarios en los activos de información para identificar la acumulación de privilegios?

29	RCD02. ¿Se revisa los derechos de acceso de los empleados, terceros a la información y a los activos que procesan la información en la culminación del contrato de trabajo o al realizarse un cambio significativo?
30	RCD03. ¿Existen un proceso de ajuste de derechos de acceso?
31	ISS01. ¿La organización cuenta con procedimientos seguros de inicio de sesión?
32	ISS02. ¿Para entornos Linux, el inicio de sesión se lo realiza mediante consola?
33	ISS03. ¿Los inicios de sesión se realizan con el usuario root?
34	SGC01. ¿Existe alguna política de gestión de contraseñas seguras de usuario que contemple factores como longitud mínima, evitar reutilización de contraseñas, reglas de complejidad?
35	CCF01. ¿Existe restricciones de acceso de algún tipo al código fuente de las aplicaciones software?
36	CCF02. ¿Se almacenan y analizan los registros de acceso y cambios en el código fuente?
37	PCC01. ¿Se dispone de una política que regule el uso de controles criptográficos para la protección de la información?
38	PCC02. ¿Los discos se encuentran encriptados?
39	PCC03. ¿Se emplea herramientas confiables para encriptar los discos?
40	PCC04. ¿Se realizan respaldo de información antes de encriptar los discos?
41	GTC01. ¿Existe una política de gestión de claves criptográficas en todo su ciclo de vida?
42	MTE01. ¿Existe algún plan de actualizaciones críticas de sistemas operativos?
43	MTE02. ¿Existe algún plan de actualizaciones de seguridad de sistemas operativos?
44	MTE03. ¿Existe algún plan de actualizaciones de seguridad de software de terceros?
45	MTE04. ¿Existe algún plan de actualizaciones de seguridad de software desarrollado por la organización?
46	GCP01. ¿Se realiza un monitoreo de los recursos del servidor para detección de ataques?
47	GCP02. ¿Se realiza un control de las configuraciones de las aplicaciones que pueden generar degradar un servicio?
48	SAM01. ¿Se encuentra definidos y separados los ambientes de desarrollo, pruebas y operativos con el objetivo de reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional?
49	GTM01. ¿Existen controles implementados para la detección, prevención y recuperación ante incidentes de malware a la seguridad informática y que sean utilizados para crear una conciencia de seguridad en los usuarios?
50	GTM02. ¿Se encuentra implementado un sistema de detección de intrusos?
51	GTM03. ¿Existe algún control que proteja contra ataques de día cero?
52	GTM04. ¿Existe algún control que proteja contra amenazas conocidas?
53	GTM05. ¿Se evidencia la existencia de controles de antivirus de programados en todos los activos de información relevantes?
54	GTM06. ¿Las bases de datos de antivirus se actualizan automáticamente?
55	CRI01. ¿La organización cumple con la política de copias de seguridad, que detalla procesos de realización de respaldos de la información?
56	CRI02. ¿La organización cumple con la política de copias de seguridad, que detalla procesos de realización de imágenes de los sistemas?
57	CRI03. ¿La organización cumple con la política de copias de seguridad, que detalla procesos de validación de información antes de dirigirse a su custodia?
58	CRI04. ¿Se realizan copias de seguridad de las configuraciones de los activos críticos?
59	RGE01. ¿Existe una correcta gestión de los archivos de registro (logs) y su posterior análisis?
60	PIR01. ¿Los archivos de registro se encuentran respaldados y protegidos, contra posibles alteraciones y accesos no autorizados?
61	RAO01. ¿Las actividades del administrador, operador del sistema se encuentran registrados y protegidos para su posterior revisión?
62	SYR01. ¿Los relojes de todos los sistemas de procesamiento de información se encuentran sincronizados a una única fuente?
63	IOS01. ¿Existen procedimientos que incluyan pruebas, aprobación para controlar la instalación de software en los sistemas operativos que comprometan la seguridad de la información?

64	IOS02. ¿Existe evidencia que no se utilice software sin soporte?
65	GTV01. ¿Se realizan escaneo de vulnerabilidades de forma regular o planificada?
66	GTV02. ¿Se realizan escaneo de vulnerabilidades después de corregir brechas de seguridad?
67	GTV03. ¿Existen un plan de respuesta ante vulnerabilidades técnicas descubiertas en los activos de información?
68	GTV04. ¿Se encuentra documentado de manera formal la aprobación o rechazo de implementación de parches de seguridad asociado a vulnerabilidades?
69	RIS01. ¿Existen controles que prohíben instalar software por parte de los usuarios?
70	ASI01. ¿Existen planes de auditoría en los que se contemple los requisitos y actividades a realizar para la verificación de sistemas de información?
71	PPR01. ¿Existe documentos formales en los que conste los requisitos de seguridad de la información requeridos por los activos de la organización con el afán de mitigar los riesgos por parte de proveedores y terceros?
72	TAP01. ¿Están establecidos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información?
73	SRP01. ¿La organización hace seguimiento, revisa y audita las configuraciones de los servicios prestados por proveedores?
74	GTP01. ¿Al realizar cambios en las configuraciones de los servicios que prestan los proveedores, se analiza con la política de la seguridad de la información?
75	ESI01. ¿Se comunica al jefe departamental las notificaciones de eventos de seguridad de la información empleando los canales de administración adecuados?
76	DSI01. ¿Existe algún mecanismo mediante el cual se exija notificar acerca de sospechas de debilidad en la seguridad de la información en los sistemas o servicios que son utilizados por los empleados como externos de la organización?
77	EES01. ¿Se evalúan los eventos repetitivos de seguridad de la información y existe alguna clasificación como incidentes / problema?
78	AIS01. ¿Se lleva un registro del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro?
79	REV01. ¿La organización tiene definido procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia?
80	VRE01. ¿Existe la verificación periódica de los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas?
81	DIP01. ¿Las instalaciones de procesamiento de datos cuentan con redundancia suficiente para ser usadas en caso de una contingencia?
82	IRL01. ¿Se cumple con la adopción de la norma ISO 27002:2013 para la seguridad de la información como se encuentra establecido en la Constitución del Ecuador?

APENDICE B. Equipo de juicio de expertos.

ID	TÍTULO	EXP.	FORMACIÓN
JE01	Ing. informático, Magíster en evaluación y auditoría de sistemas tecnológicos.	6 años	Design thinking innovation of products and services, Strategy model CANVAS - SMC, Packetlight networks certified systems engineer WDM solutions, Sistemas de gestión de seguridad de la información – norma ISO 27001:2013, Taller de gestión de incidentes de seguridad informática, Dirección de gestión de proyectos, ITIL 2011 Fundamentos, COBIT 5 Fundamentos, Liderazgo para gerentes de proyectos
JE02	Ingeniero en tecnologías de la información.	7 años	Microsoft Office Specialist, Administración Linux básico, Administración Linux avanzado, Administración de servicios de red en Linux, VMWARE VSPHERE: install, configure, manage [v5.5], VMWARE VSPHERE: install, configure, manage [v6.5], VMWARE VCENTER OPERATIONS MANAGER: analyze and predict [v5.x]
JE03	Ingeniero de sistemas, Magíster en telemática.	3 años	Career development 2x: communication and teamwork, Fortinet bundle 201-fortigate multi-threat security systems i & 301 fortigate multi-threat security systems ii, Curso nokia: sr-os services implementation, Curso avanzado de ipv6, Curso introductorio a ipv6, Gpon 2nd line maintenance training & imanager u2000 training, Administración de proyectos.